

Las Aventuras de
Quirquincho©
#4
Chaucha Ediciones

Las Aventuras de

Quirquincho©



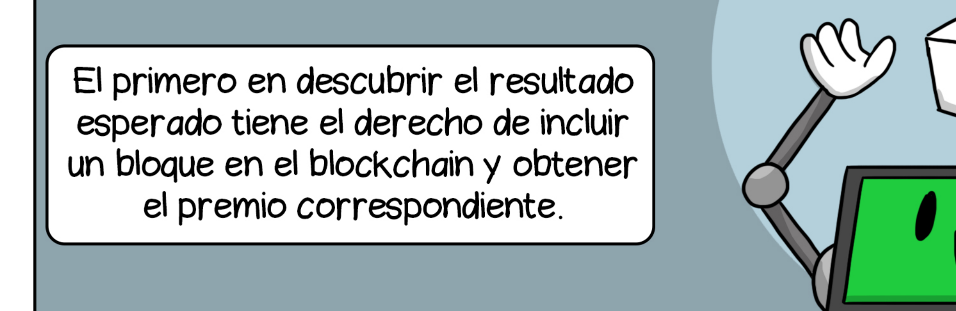
Historia: Camilo Castro (@clsource)
Ilustraciones: Leo Quezada (@leo8bits)

16 de Marzo de 2018

El pirquinero le pidió ayuda a Quirquincho a llevar sus capachos.

Hicieron una pequeña carrera hacia la ciudad y el pirquinero le regaló un recuerdo de Andacollo a Quirquincho por su buena onda.

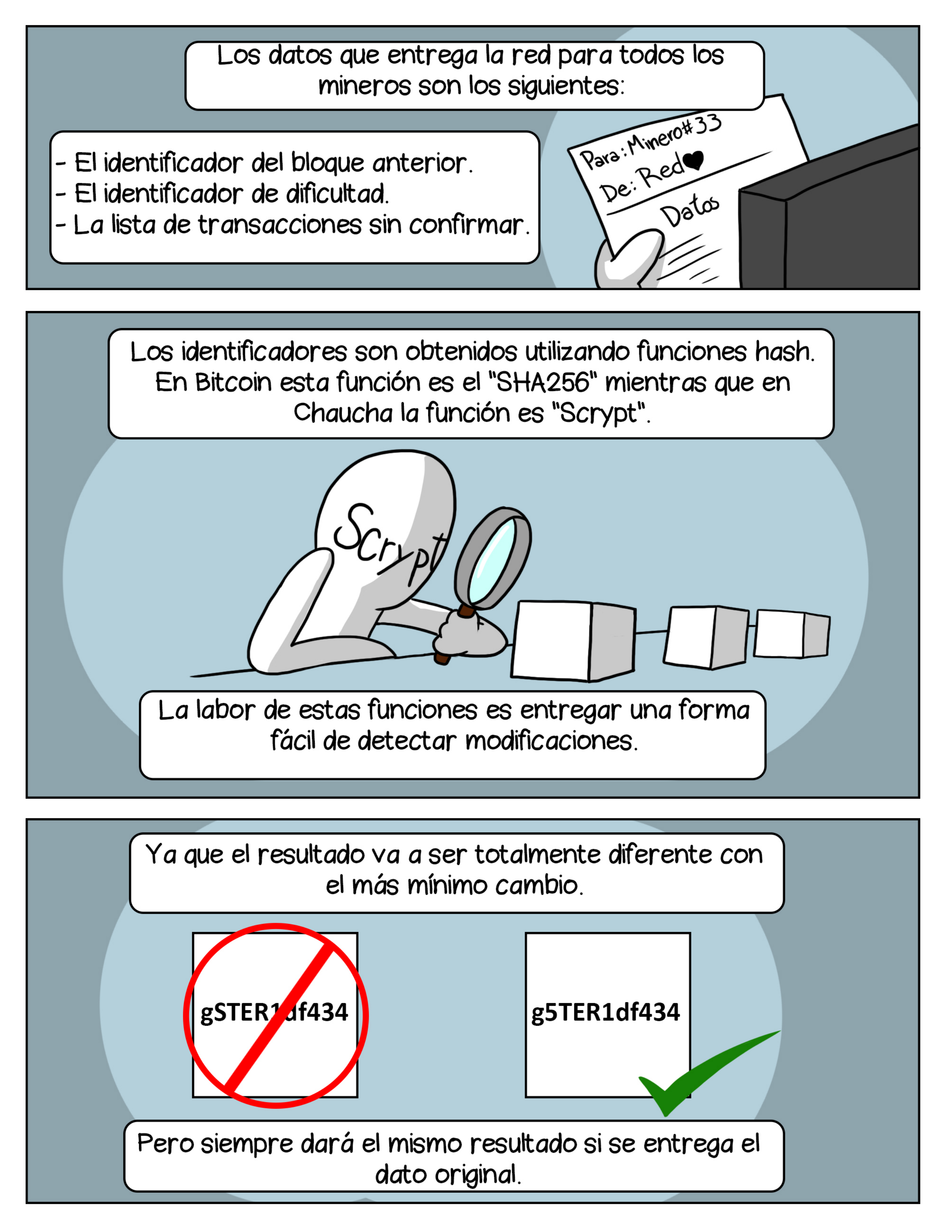






En ese momento todos los mineros desechan el bloque que estaban haciendo y comienzan a crear uno nuevo, utilizando los últimos datos.

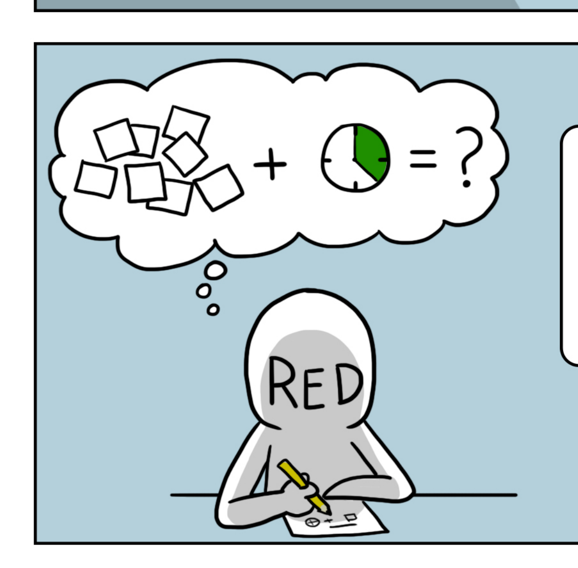
Basura



Los datos que entrega la red para todos los mineros son los siguientes:
- El identificador del bloque anterior.
- El identificador de dificultad.
- La lista de transacciones sin confirmar.
Para: Minero#33
De: Red
Datos
Los identificadores son obtenidos utilizando funciones hash. En Bitcoin esta función es el "SHA256" mientras que en Chaucha la función es "Scrypt".
Scrypt
La labor de estas funciones es entregar una forma fácil de detectar modificaciones.
Ya que el resultado va a ser totalmente diferente con el más mínimo cambio.
gSTER1df434
g5TER1df434
Pero siempre dará el mismo resultado si se entrega el dato original.

El identificador de dificultad es la pieza clave que permite saber si un bloque ganó la competencia y puede ser incluido en el blockchain.



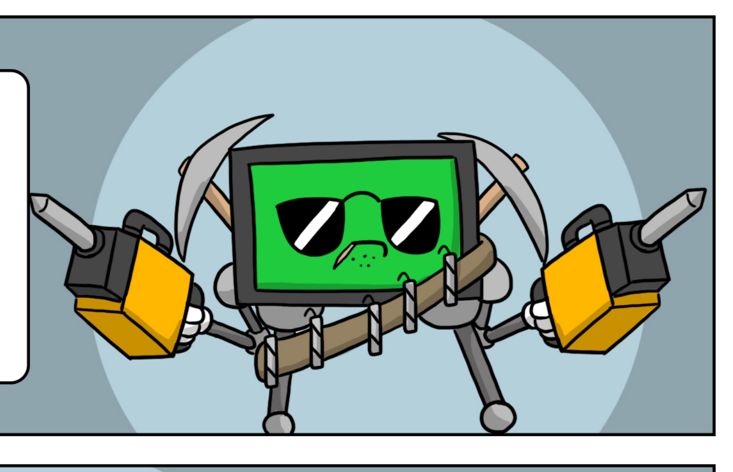


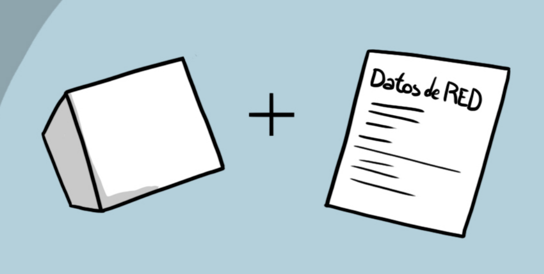
Es generado automáticamente por la red dependiendo de distintos factores como la cantidad de bloques anteriores y el tiempo en que tomaron en ser incluidos.

Puede ser un número grande o un número pequeño y variará constantemente.
Mientras más pequeño es el número de este identificador, más difícil será encontrar un número menor.

Dificultad
600
500
400
300
200
100
1 Día
2 Días
3 Días
4 Días
5 Días
6 Días
7 Días

Los mineros utilizan todo su arsenal de procesamiento para encontrar un identificador de bloque que sea menor al identificador de dificultad.

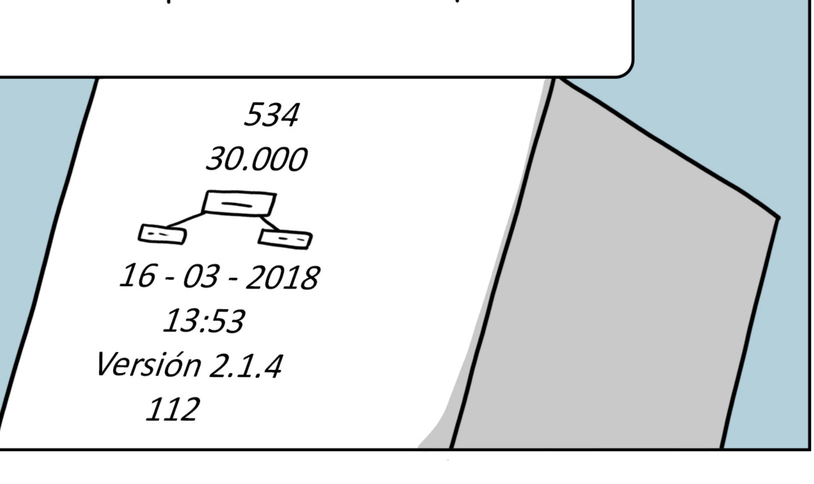




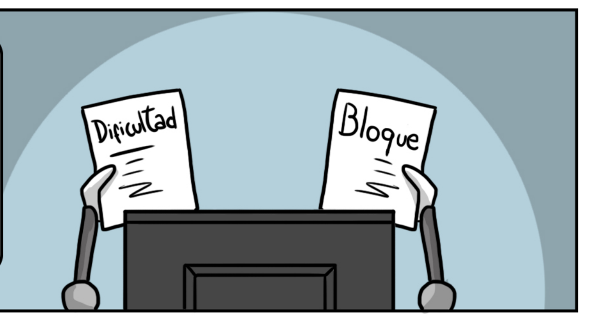
Este identificador de bloque es obtenido juntando los datos otorgados por la red con los datos propios de cada bloque.

En total un bloque tiene los siguientes datos:

- El identificador del bloque anterior
- El identificador de dificultad
- El identificador de las transacciones incluidas (Merkle Root)
- La fecha y hora de creación del bloque
- La versión de las reglas usadas para validar el bloque
- Un número aleatorio



Los mineros unen todos estos datos y aplican la función hash para obtener el identificador del bloque. Luego comparan este hash con el identificador de dificultad.



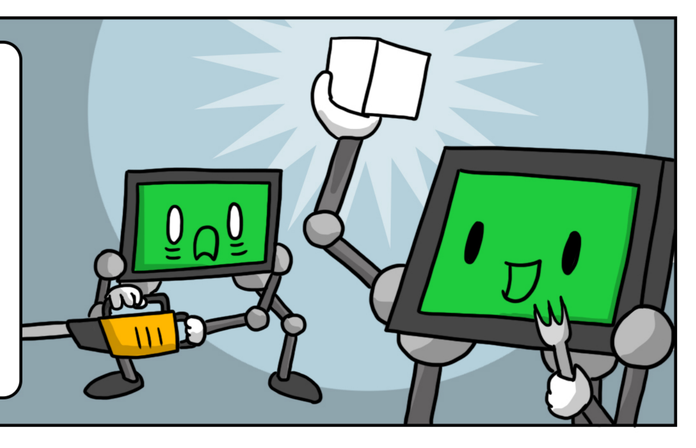
Si el valor es menor han ganado y la red anuncia que se ha incluido un nuevo bloque.

RED

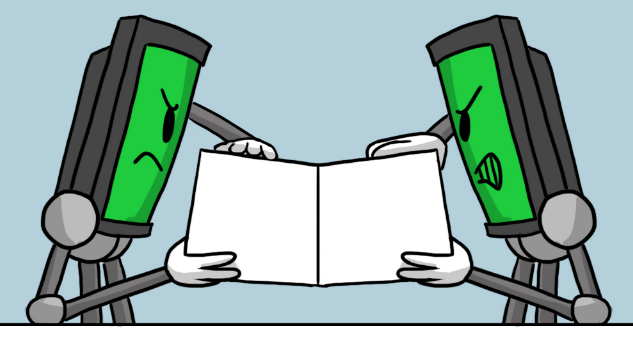
¡Hay bloque nuevo!

Este proceso toma tiempo y deben probar millones de distintas combinaciones. Variando el número aleatorio, la fecha o el identificador de transacciones.

Es en esta labor donde ocupan casi toda la capacidad de procesamiento.
Aunque de ves en cuando algún minero con poca capacidad de procesamiento igual puede achuntarle al identificador ganador.



En ocasiones dos o más mineros encuentran un identificador ganador casi al mismo tiempo.
Lo que obliga a todos a decidir qué bloque debe ser considerado como oficial.





Las Aventuras de

Quirquincho©



Las Aventuras de

Quirquincho©



www.chaucha.cl

